Foundation of Cryptography, Fall 2011

Rotem Arnon

December 15, 2011

Question 2

1. Let $f : \{0,1\}^n \to \{0,1\}$ be $f(x) = 0$. Given any $y \in \{0,1\}$ either y has no preimage, or 0^n is its preimage, therefore it is easy to find a preimage - always return 0^n. On the other hand, at least intuitively, given $f(x)$, the only way to find x itself is to randomly guess it according to U_n. The probability that A and a sample x chosen at random according to U_n are the same is:

$$\Pr[A(1^n, f(U_n)) = U_n] = \Pr[A(1^n, 0) = U_n] = 2^{-n} = neg(n)$$

   f is **not** a one way function by definition.

2. Assume in contradiction that there exists a polynomial $p \in$ poly and an infinite set $I \subset \mathbb{N}$ such that $\mathbb{E}[cyc_f(U_n)] < p(n)$ where f is an α-one way function. Consider the following inverter for f, A: given the input $1^n, y \in f(U_n)$, A calculates $f(y), f(f(y))$ etc. until $f^i(y) = y$ or until $i = \frac{1}{1-\alpha(n)} \cdot p(n)$. If $f^i(y) = y$ the output is $f^{i-1}(y)$ and otherwise the inverter fails. The probability that the inverter fails is equal to the probability that $cyc_f(y) \geq \frac{1}{1-\alpha(n)} \cdot p(n)$. Using our assumption that $\mathbb{E}[cyc_f(U_n)] < p(n)$ and Markov inequality we get

$$\Pr\left[cyc_f(U_n) \geq \frac{1}{1-\alpha(n)} \cdot p(n)\right] \leq \Pr\left[cyc_f(U_n) \geq \frac{1}{1-\alpha(n)} \cdot \mathbb{E}[cyc_f(U_n)]\right] \leq 1 - \alpha(n)$$

   and therefore the probability that the inverter A inverts f correctly is $\Pr\left[A(y) \in f^{-1}(U_n)\right] > \alpha(n)$. A is a PPT algorithm since the number of rounds i is polynomial and f itself is polynomial-time computable function, and it inverts f with high enough probability, in contradiction to the fact that f is an α-one way function.

3. let $f : \{0,1\}^\star \to \{0,1\}^\star$ be $f(x) = x + 1$. f is an efficiently computable function and $\mathbb{E}[cyc_f(U_n)]$ is not polynomial bounded (since $\mathbb{E}[cyc_f(U_n)] = \infty$). f is not a weakly one way function (it is easy to invert the function). Moreover, for the same function $\underset{x}{min}(cyc_f(x))$ is not polynomial bounded as well. Another example: if a function from $\{0,1\}^\star$ to $\{0,1\}^\star$ is not constructive, we can use $g : \{0,1\}^n \to \{0,1\}^n$ where $g(x) = x + 1$ for all $x \neq 1^n$ and $g(1^n) = 0^n$. This function has one cycle of size 2^n and therefore both $\mathbb{E}[cyc_g(U_n)]$ and $\underset{x}{min}(cyc_g(x))$ are not polynomial bounded, but g is not a weakly one way function.